

Date: June 21, 2026

MEMORANDUM ON

City of Hamilton's Interim Control By-law For
Datacentre Development

SUBJECT:	Systemic Risks and Policy Recommendations for Datacentres in Hamilton
IN RESPONSE TO:	Interim Control By-law Datacentre Development
FROM:	B. Bhardwaj
TO:	City of Hamilton, ON, Canada

The Purpose

The City of Hamilton has passed a datacentre moratorium and is now preparing an Interim Control By-law (ICBL) and a corresponding Datacentre Framework. This memo serves as a Risk-to-Policy Map to support City staff in being aware and intentional throughout the drafting of the ICBL and the development of the Framework. While the recommendations listed in this document are specifically drafted for ICBL, they can be considered as future amendments to other By-laws. This document maps risk findings for hyperscale datacentre proposals to specific policy actions the City can take under its jurisdiction, including zoning, by-laws, building permits, noise, traffic, stormwater, and transparency requirements. It ensures that the City's response is **evidence-based, people-first, and legally defensible**.

For risks the City identifies as beyond its direct jurisdiction, this memo specifies how the City can use municipal tools like zoning and Official Plan amendments, Municipal Act s.157 advocacy, Climate Lens and Carbon Budget Framework, stormwater and local water by-laws, and OLT consolidation strategies to:

- prohibit datacentres entirely while studying infrastructure, energy, water, and environmental capacity;
- request regulatory interventions;
- apply a climate lens to show datacentres would undermine Hamilton's climate targets;
- control local aspects of water balance and stormwater;

- support community decisions through formal submissions, advocacy, and coordinated intergovernmental action.

This approach ensures the City's response is aligned with the Provincial Planning Statement (PPS) and strengthens the City's position in any Ontario Land Tribunal (OLT) proceedings.

SECTION 1: Risk Categories and Policy Triggers

This section organizes the 20 identified hyperscale data centre risks into four categories and specifies the **policy triggers** that activate municipal tools. A policy trigger is a condition or threshold that requires staff to apply a specific control, condition, or prohibition.

Category 1: Land Use, Zoning, and Physical Impacts

These risks are high-priority and directly controllable by the City through zoning, by-laws, and permitting.

Risk	Municipal Policy Trigger	Policy Action (What the City Does)
Land-Use Conflict	Proposal in any zone, including M5 General Industrial	Prohibit datacentres in all zones via ICBL; update Zoning By-law 05-200 to explicitly exclude the use
Noise (Backup Generators)	Generator testing >X hours/month, noise >Y dB at property line	Enforce noise by-law; limit generator testing frequency/duration; require acoustic enclosures and setbacks
Traffic/ Trucking	Construction or delivery traffic exceeding municipal thresholds	Require traffic impact study; set truck routes, delivery hours, construction hours, and staging limits
Emergency Response Capacity	Facility size or hazard level requiring specialized response	Require on-site emergency plan; coordination with fire/police; 24/7 staffing and training
Waste Heat Rejection	Heat discharge affecting neighbourhood or exceeding property-line limits	Zoning conditions on cooling systems; heat limits at property line; siting restrictions
Water-Balance Impact	On-site water use or stormwater discharge exceeding local thresholds	Require stormwater management plan; on-site water re-use; local discharge limits

E-Waste Toxicity	Decommissioning or hazardous waste generation	Apply waste management by-laws; require decommissioning plan and hazardous waste handling
Diesel Generator Emissions	Backup generator use or fuel storage	Enforce local by-laws on generator use, testing frequency, fuel storage, and on-site controls
PFAS (“Forever Chemicals”)	Cooling water treatment or discharge	Require cooling water treatment conditions; discharge limits and reporting

Principle:

Any proposal that meets or exceeds these thresholds must be prohibited under the ICBL unless the City has a complete Framework with enforceable conditions. The ICBL must include a no-exceptions clause that blocks all data centre uses, regardless of size, name, or power source.

Category 2: Transparency, Accountability, and Public Participation (Municipality)

These risks relate to governance failures that the City can directly fix through policy and procedural controls.

Risk	Policy Trigger	Policy Action
Transparency Deficits (NDAs)	Any attempt to use NDAs, side letters, or confidential agreements for data centre development	Ban NDAs for data centre deals; require public disclosure of all agreements, incentives, and impact assessments
Community Benefits	Proposal seeking public support, land, or incentives	Require binding community benefit agreements; local hiring, training, and supplier commitments; third-party verification
Independent Verification	Any application for permits or approvals	Require third-party audits for noise, water, energy, emissions, and safety as pre-conditions for permits

Principle:

No data centre application may proceed without full public transparency, binding community benefits, and verified impact data. The ICBL must explicitly state that no confidential dealings are permitted and that all agreements must be posted on a public Data Centre Study Register.

Category 3: Environmental, Energy, and Infrastructure Risks (Beyond Municipal Jurisdiction)

These risks are high-impact but largely outside municipal control, requiring provincial/federal/utility intervention. The City's role is to document, escalate, and advocate.

Risk	Policy Trigger	Next Step (Municipal Act s.157)
Electricity Demand	Proposal $\geq$ X MW continuous load	Submit formal concerns to IESO/utility/provincial ministry; request load review and capacity assessment
Grid Stability	Large-load integration without grid study	Request provincial grid stability review; advocate for interconnection limits
Water Consumption	Regional water withdrawal exceeding watershed capacity	Submit concerns to provincial ministry/watershed agency; request water allocation review
Emissions Disclosure (GHG)	Facility with significant GHG emissions	Request provincial/federal emissions reporting and climate compliance review
Public Funds Redirection	Proposal seeking tax breaks, subsidies, or infrastructure support	Notify provincial/federal governments of net cost to municipality; advocate for removal of incentives
Supply Chain Vulnerabilities	Dependence on global hardware/logistics	Document risks; submit concerns to provincial/federal trade and infrastructure ministries
Cybersecurity	Facility handling sensitive data or critical infrastructure	Request federal/provincial cybersecurity standards and incident-response requirements
CapEx Wall / Valuation Crash	Project dependent on speculative AI monetization	Document financial risk; advise Council and provincial partners of long-term infrastructure risk

Principle:

When a risk is identified as beyond municipal jurisdiction, staff must:

1. **Document the risk** in the ICBL justification and Framework.
2. **Escalate formally** using Municipal Act s.157 tools (submissions, letters, joint requests).
3. Advocate for regulatory intervention at provincial/federal levels.

4. **Support community decisions** by ensuring residents have clear information about jurisdictional gaps.

Category 4: Moratorium and No-Exceptions Enforcement (Municipality)

This category ensures the ICBL itself closes all loopholes and enforces a true “no exception whatsoever ever” moratorium.

Risk	Policy Trigger	Policy Action
Misclassification	Proposal labeled as “manufacturing”, “office”, “warehouse”, “R&D”, or “private power generation”	Define “data centre” functionally in Zoning By-law 05-200; prohibit all uses whose primary purpose is data centre activity
Mixed-Use / Phased Development	Small Phase 1 with large future phases; mixed-use with server component	ICBL prohibits all phases, expansions, campuses, and mixed-use data centre components.
Off-Grid / Private Power	Proposal using private generation or off-grid power	ICBL prohibits datacentres regardless of power source; blocks private generation for datacentres.
Back-Door Approvals	Use of minor variances, consents, or other appeals to bypass moratorium	ICBL prohibits all related approvals (building permits, zoning amendments, minor variances, site plan approvals, consents).

Principle:

The ICBL must include an explicit **no-exceptions clause** that:

- states there are no exemptions, grandfathering, or transitional approvals;
- says no implied exceptions;
- prohibits any use that functions as a data centre, regardless of name, size, phase, or power source;
- and states that if one provision is invalid, the moratorium remains in force.

Addressing Risks Beyond City Jurisdiction (Category 3)

The City staff must document, escalate, and advocate, using municipal tools to address these risks and strengthen the OLT case:

- **ICBL under Planning Act s.38:** Prohibit datacentres entirely while studying whether the municipality has the infrastructure, energy, water, and environmental capacity to support them.

- **Zoning By-law 05-200 updates:** Explicitly prohibit datacentres in all zones, including M5.
- **Official Plan amendments:** Add policy that datacentres are not supported unless Category 3 risks are resolved.
- **Municipal Act s.157 advocacy:** Escalate concerns to provincial/federal authorities and request regulatory interventions (grid studies, water allocation reviews, emissions reporting, removal of incentives).
- **Climate Lens and Carbon Budget Framework:** Apply Hamilton's Climate Action Strategy to show datacentres would undermine climate targets and exceed the carbon budget.
- **Stormwater and local water by-laws:** Control local water-balance and stormwater impacts at the property line.

This ensures the City is not ignoring Category 3 risks, but actively coordinating with provincial and federal partners to ensure infrastructure, energy, water, and environmental safeguards are met.

For a moratorium enforcement, the ICBL must close all loopholes with a no-exceptions clause that blocks:

- misclassification (e.g., “manufacturing”, “office”, “warehouse”, “R&D”, “private power generation”),
- mixed-use and phased development,
- off-grid and private power systems,
- back-door approvals (minor variances, consents, site plan approvals, zoning amendments).

It's important that the clause explicitly states:

- there are no exemptions, grandfathering, or transitional approvals;
- there are no implied exceptions;
- the prohibition applies to all uses whose primary purpose is data centre activity, regardless of name, size, phase, or power source;
- and if one provision is invalid, the moratorium remains in force.

Section 2: Recommendations for M5 Zoning By-law 05-200 Updates for Hyperscale Datacentres

1. Add a Standalone “Datacentre” Definition in Section 2 (Definitions)

M5 does not define “datacentre,” “hyperscale datacentre,” or “AI datacentre.”

Recommendation: Add this definition to Section 2 of Zoning By-law 05-200:

“Data Centre” means a building, structure, or use whose primary purpose is to:

- house, operate, or maintain computer servers;
- operate networking equipment;

- store, process, or manage data;
- run digital processing equipment; or
- provide related infrastructure for these activities,

whether operated as a standalone use or as part of another principal use, and regardless of size, capacity, or technology type (including AI, cloud, high-performance computing, or similar uses).

“Hyperscale Data Centre” means a datacentre with a continuous electrical load of 10 MW or greater, or a server floor area of 5,000 m² or greater, or water use of 300,000 gallons/day or greater.

Why:

- Prevents developers from arguing datacentres are “manufacturing,” “office,” or “warehouse.”
- Captures AI, cloud, HPC, and related infrastructure, and establishes clear thresholds for hyperscale.

2. Add “Data Centre” to Section 9.5.2 (Prohibited Uses in M5)

M5 Section 9.5.2 lists prohibited uses, but “data centre” is not included.

Recommendation: Add Prohibited Uses in M5 Section 9.5.2:

- Datacentre (including hyperscale datacentre, AI datacentre, cloud datacentre, high-performance computing facility)
- Any use whose primary purpose is datacentre activity, regardless of name or classification

Why:

- Explicitly prohibits datacentres in M5, even as accessory uses.
- Blocks misclassification under “manufacturing,” “office,” “warehouse,” “R&D,” or “private power generation facility.”

3. Add a “No Misclassification” Clause in Section 9.5 (M5 General Provisions)

Currently, developers can label datacentres as other permitted uses.

Recommendation: Add a *No Misclassification* clause to Section 9.5:

No building, structure, or use whose primary purpose is data centre activity shall be classified as:

- manufacturing;
- industrial administrative office;
- warehouse;
- research and development establishment;
- private power generation facility;

- or any other permitted use in M5.

Why:

- Closes the loophole where developers hide datacentres under permitted use names, and ensures primary purpose determines the use, not the label.

4. Add Hyperscale Thresholds as Additional Prohibitions in Section 9.5.2

M5 does not distinguish between small and hyperscale facilities.

Recommendation: Add Additional Prohibitions for Hyperscale in Section 9.5.2:

- Any datacentre meeting or exceeding **hyperscale thresholds** (≥ 10 MW continuous load, $\geq 5,000$ m² server floor area, or $\geq 300,000$ gallons/day water use) is prohibited in M5.
- Any proposal that includes future phases or expansions that would result in hyperscale thresholds is prohibited.

Why:

- Prevents “small Phase 1” strategies that expand to hyperscale later.
- Blocks phased development and campus strategies.

5. Add Distance and Buffer Requirements (If Any Smaller Datacentres Are Ever Allowed)

M5 has no minimum distance requirements for industrial uses near sensitive areas.

Recommendation: Add Minimum Distance Requirements to Section 9.5 if datacentres are ever permitted in any zone:

- Datacentres must be at least **500 metres** from residential zones, schools, hospitals, and daycares.
- Datacentres must have a **30-metre buffer** with landscaping and acoustic barriers from residential or institutional properties.

Why:

- Even if datacentres are prohibited, this prepares M5-200 for future policy.
- Prepares M5 for future policy where smaller datacentres might be allowed under strict conditions.
- Protects people and neighbourhoods from noise, heat, and traffic impacts.

6. Add Noise and Generator Testing Limits in Section 9.5.4 (Performance Standards)

M5 has general industrial performance standards, but no specific generator testing or noise limits for datacentres.

Recommendation: Add *Noise and Generator Testing Limits* to Section 9.5.4:

- Quantify safe maximum noise at property line at daytime and nighttime.
- Backup generator testing, for example maximum 4 hours per month, maximum 2 hours per test, during 8:00 AM–6:00 PM weekdays only.
- All generators must have acoustic enclosures and be located at least **1km from residential or institutional properties**.

Why:

- Directly addresses noise risk from backup generators and limits disruptive testing frequency and duration.

7. Add Stormwater and Water-Balance Requirements in Section 9.5.5 (Site Development Standards)

M5 has general stormwater standards, but no datacentre-specific requirements.

Recommendation: Add *Stormwater and Water-Balance Requirements* to Section 9.5.5:

- Datacentres must provide a stormwater management plan demonstrating no adverse impact on local drainage.
- On-site water re-use must meet minimum 50% re-use of total water demand.
- Discharge at property line must not exceed local water-balance capacity.

Why:

- Addresses water-balance risk at the municipal level.
- Requires re-use and discharge limits.

8. Add Emergency Response and Fire Safety Requirements in Section 9.5.6 (Safety Standards)

M5 has general safety standards, but no datacentre-specific emergency response requirements.

Recommendation: Add *Emergency Response and Fire Safety Requirements* to Section 9.5.6:

- Datacentres must provide an on-site emergency response plan coordinated with Hamilton Fire and Police.
- Datacentres must have **24/7 staffing** with trained emergency response personnel.
- Datacentres must provide fuel storage and chemical handling plans meeting municipal safety standards.

Why:

- Addresses emergency response capacity risk.
- Ensures coordination with local emergency services.

9. Add Transparency and NDA Prohibition in Section 9.5.7 (Public Disclosure)

M5 has no transparency requirements for industrial uses.

Recommendation:

Add *Transparency and NDA Prohibition* to Section 9.5.7:

- No non-disclosure agreements (NDAs), side letters, or confidential agreements are permitted for data centre development.
- All agreements, incentives, impact assessments, and design documents must be publicly posted on the City's website.
- A public Data Centre Study Register must be maintained with all reports, meeting notes, and decisions.

Why:

- Addresses transparency deficits and NDAs by ensuring public accountability and legibility.

10. Add “No Exceptions” Clause in Section 9.5.8 (General Provisions)

M5 has no explicit prohibited uses.

Recommendation: Add *No Exceptions Clause* to Section 9.5.8:

- There are no exemptions, grandfathering rights, or transitional approvals for datacentres in M5.
- No implied exceptions exist.
- The prohibition applies to all datacentres, regardless of name, size, phase, mixed-use status, or power source (including off-grid or private power).
- If any provision is found invalid, the datacentre prohibition remains in force.

Why:

- Closes all loopholes for misclassification, mixed-use, phased development, off-grid systems, and back-door approvals.
- Ensures the prohibition is truly “no exception whatsoever ever.”

Addressing Other By-Law Gaps

11. Zoning By-law 05-200, Other Industrial Zones (M1, M2, M3, M4)

Currently, like M5, other industrial zones (M1, M2, M3, M4) also do not explicitly prohibit datacentres.

- It allows developers to locate hyperscale datacentres in any industrial zone, not just M5, creating a gap to prohibit in M5 but allow in M1–M4.

Add datacentre definitions and prohibitions to all industrial zones (M1, M2, M3, M4, M5) in their respective prohibited use sections.

12. Zoning By-law 05-200, Employment Areas and Business Parks

Employment areas and business park zones (e.g., EB, EP zones) do not explicitly prohibit datacentres.

- Developers can propose datacentres in business parks near employment areas, not just traditional industrial zones. This bypasses M5-specific restrictions.

Add datacentre conditions, if not prohibitions) to all employment and business park zones.

13. Zoning By-law 05-200, “Primary Purpose” Test

The by-law does not include a “primary purpose” test to determine whether a use is a data centre.

- Developers can claim datacentre activity is accessory to another permitted use (e.g., “office with some servers”) to avoid the data centre definition by calling it “accessory use.”

Add a clause: “No building, structure, or use whose primary purpose is data centre activity shall be classified as any other permitted use, regardless of name or accessory status.”

14. Zoning By-law 05-200, No Phase or Campus Prohibition

The by-law does not prohibit phased development or multi-building campuses that would result in a data centre.

- Developers propose Phase 1 as “small” and plan future phases to reach hyperscale.
- They propose campuses with multiple small buildings that together function as a data centre.

Add “Any proposal that includes future phases or expansions that would result in a data centre (including hyperscale thresholds) is prohibited. Multi-building campuses whose combined purpose is data centre activity are prohibited.”

15. Zoning By-law 05-200, No Waterfront, Urban or Rural, Non-industrial, Light or Extractive Industrial, Settlement or Local or Arterial Commercial,

Community Institutional & All Other Zoning Prohibitions

The by-law does not explicitly prohibit datacentres based on defined zones regardless of the classification, each zone must prohibit datacentres at least during the moratorium so these gaps don't result in exceptions.

- Developers may navigate these gaps in by-laws that don't explicitly prohibit datacentres, and can use private it to bypass the moratorium.

Add “The prohibition applies to all datacentres, regardless of power source (including off-grid, private power generation, or microgrid systems).”

16. Traffic By-law, No Datacentre Traffic Impact Study Requirement

Hamilton's Traffic By-law does not require traffic impact studies specifically for datacentres.

- Developers don't have to assess construction traffic, delivery trucks, or employee vehicle impacts.
- No truck route, delivery hour, or staging controls.

Add a requirement “Data centre proposals must provide a traffic impact study and comply with truck routes, delivery hours, construction hours, and parking/staging limits.”

17. Official Plan Doesn't Have Datacentre Policy Language

Hamilton's Official Plan does not include policy language on datacentres or hyperscale facilities.

- No land-use policy stating datacentres are not supported unless infrastructure, energy, water, and environmental risks are resolved.

Add Official Plan policy: “Datacentres, including hyperscale datacentres, are not supported unless the City confirms electricity capacity, grid stability, water allocation, GHG emissions within climate targets, and emergency response capacity.”

18. Committee of Adjustment Zones' Have No Datacentre Minor Variance Prohibition

The Committee of Adjustment can grant minor variances that bypass zoning restrictions, and there's no prohibition on data centre minor variances.

- Developers apply for minor variances to bypass distance, buffer, or size restrictions. (as seen in Case Study 1: Steelpoint Severance Application B-2026-00011) This is a back-door approval route.

Add “No minor variances, consents, site plan approvals, or zoning amendments for datacentres are permitted under the ICBL moratorium” to both ICBL and zoning.

Section 3: Sample Proponent Questionnaire

A Proponent Questionnaire should force specificity, leaving no room for negotiations and exceptions. The City must know the answers to the questions including (but not limited to) the following before considering the proposal complete:

- Why must this be in a city, rather than an industrial, exurban, or rural site?
- What alternative sites were considered, and why were they rejected?
- How much electricity will the facility require at buildout, and in each growth phase?
- What is the expected peak and average water demand, and what cooling system is proposed?
- Will all water use be metered, publicly reported, and billed at full cost?
- What backup generation is proposed, for how long, and what emissions and noise will it create?
- What is the maximum sound level at the property line and nearest residences?
- What heat rejection or waste-heat impacts are expected nearby?
- What stormwater, wastewater, and fire-flow infrastructure is required?
- What community benefits are proposed, and are they contractually binding before permits?
- What cyber, physical security, and emergency response plans exist?
- What specific local jobs, local procurement, and training commitments are guaranteed?
- Will the proponent accept public reporting on energy, water, outages, and complaints?
- What happens if provincial power or water constraints change after approval?
- Will the company agree to a moratorium-triggered stop-work or review clause if local thresholds are exceeded?